An explicit class of codes with good parameters and their duals

Özbudak, Ferruh; Ling, San; Xing, Chaoping

2005

Ling, S., Xing, C., & Özbudak, F. (2005). An explicit class of codes with good parameters and their duals. Discrete Applied Mathematics, 154(2), 346-356.

https://hdl.handle.net/10356/96321

https://doi.org/10.1016/j.dam.2005.03.013

An explicit class of codes with good parameters and their duals

San Ling[a,1], Chaoping Xing[a], Ferruh Özbudak[b,*]

[a] *Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543, Republic of Singapore*
[b] *Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, İnönü Bulvarı, 06531, Ankara, Turkey*

Abstract

We study a class of codes with good parameters and their duals explicitly. We give direct constructions of the dual codes and obtain self-orthogonal codes with good parameters.

Keywords: Linear codes; Dual codes; Self-orthogonal codes; Optimal codes

1. Introduction

It is well known that subfield subcodes and propagation techniques would give codes with good parameters. Recently Xing, Ling and Niederreiter [8,4,5] have constructed a class of codes with very good parameters from the rational function field of $\mathbb{F}_q$ using specially chosen subcodes of Reed–Solomon codes and propagation rules. Due to their good parameters and algebraic structures, this class of linear codes has attracted further attention. For instance, a decoding algorithm of these codes is given in [6] and these codes have also been generalized to arbitrary algebraic function fields [9].

In this paper we introduce a general framework for such constructions over rational function fields and study their dual codes. Since subcodes and propagations in the construction have nice algebraic structures, it turns out that the dual codes are also in the same class and we can easily control the dual codes so that we get self-orthogonal and self-dual codes with good parameters. By codes with good parameters, we basically mean linear codes with parameters close to the best known ones according to Brouwer's table [2] or certain known bounds. We show that all linear codes can be obtained from our construction in a unique way and dual codes as well as self-orthogonality can be obtained in a simple and explicit manner. Direct constructions of the dual codes and self-orthogonal codes are provided.

This paper is organized as follows. In Section 2 we introduce our construction and consider the dual codes explicitly. We study direct constructions of dual codes in Section 3. Some self-orthogonal codes with good parameters are constructed.

* Corresponding author. Fax : +90 312 210 12 82.
E-mail addresses: matlings@nus.edu.sg (S. Ling), matxcp@nus.edu.sg (C. Xing), ozbudak@math.metu.edu.tr (F. Özbudak).
[1] This author is now with Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Block 5 Level 3, 1 Nanyang Walk, Singapore 637616, Republic of Singapore.

2. Construction

Throughout the paper we use the usual Euclidean inner product. If $C \subseteq \mathbb{F}_q^n$ is a linear code, we denote its dual by $C^\perp$. A code C is said to be self-orthogonal if $C \subseteq C^\perp$. If $C = C^\perp$, then C is said to be self-dual. For $\lambda_i \in \mathbb{F}_q \backslash \{0\}$ for $i = 1, 2, \ldots, n$, let $(\lambda_1, \ldots, \lambda_n) \cdot C$ denote the equivalent code defined as $\{(\lambda_1 c_1, \ldots, \lambda_n c_n) \mid (c_1, \ldots, c_n) \in C\}$. If $(\lambda_1, \ldots, \lambda_n) \cdot C \subseteq C^\perp$ for some $\lambda_1, \ldots, \lambda_n \in \mathbb{F}_q \backslash \{0\}$, then C is said to be quasi-self-orthogonal. Similarly, if this containment is in fact an equality, then C is quasi-self-dual. Let $\mathbb{F}_q$ be a finite field and let $\overline{\mathbb{F}}_q$ be a fixed algebraic closure.

Let r be any prime and consider the set

$$\Lambda_q^r = \{(a_1, a_2, \ldots, a_r) \mid 0 \leqslant a_i \leqslant q-1, 1 \leqslant i \leqslant r\}$$

of r-tuples of integers between 0 and $q-1$. Let Ω_r denote the cyclic group generated by the cyclic shift ω_r on Λ_q^r, i.e.,

$$\omega_r(a_1, a_2, \ldots, a_r) := (a_2, a_3, \ldots, a_r, a_1).$$

Note that $\Omega_r = \langle \omega_r \rangle \cong \mathbb{Z}/r\mathbb{Z}$. For $\mathbf{a} = (a_1, \ldots, a_r) \in \Lambda_q^r$, let $O_{\mathbf{a}}$ denote the orbit of $\mathbf{a}$ under the action of the group Ω_r on Λ_q^r

$$O_{\mathbf{a}} = \{(b_1, \ldots, b_r) = \omega_r^i(a_1, \ldots, a_r) \mid 1 \leqslant i \leqslant r\} \subset \Lambda_q^r.$$

Note that, for $\mathbf{a}' \in O_{\mathbf{a}}$, we have $O_{\mathbf{a}} = O_{\mathbf{a}'}$. We also define the associated polynomial $h_{\mathbf{a}}$ of the orbit $O_{\mathbf{a}}$ as

$$h_{\mathbf{a}} := \sum_{(b_1,\ldots,b_r) \in O_{\mathbf{a}}} x^{b_1 + b_2 q + \cdots + b_r q^{r-1}}.$$

Since r is a prime number, there are $m := (q^r - q)/r + q$ distinct orbits. Let $\mathcal{S} = \{h_1, \ldots, h_m\}$ be the set of all associated polynomials. For every $\mathbf{a} = (a_1, \ldots, a_r) \in \Lambda_q^r$, let

$$\overline{\mathbf{a}} = (q - 1 - a_1, \ldots, q - 1 - a_r).$$

Notation 2.1. For an orbit $O_{\mathbf{a}}$ of Λ_q^r under the action of Ω_r, we define $\overline{O}_{\mathbf{a}}$ as

$$\overline{O}_{\mathbf{a}} = O_{\overline{\mathbf{a}}}.$$

For $h_{\mathbf{a}} \in \mathcal{S}$, we define $\overline{h}_{\mathbf{a}} \in \mathcal{S}$ as

$$\overline{h}_{\mathbf{a}} = h_{\overline{\mathbf{a}}}.$$

Let $\mathcal{P}$ be a subset of $\mathbb{F}_{q^r}$ with the largest cardinality such that

$$\alpha \in \mathcal{P} \Rightarrow \alpha^q = \alpha \quad \text{or} \quad \alpha^{q^i} \notin \mathcal{P} \text{ for } 1 \leqslant i \leqslant r-1. \tag{2.1}$$

Then $\#\mathcal{P} = (q^r - q)/r + q = m$. Let $\mathcal{P} = \{\alpha_1, \ldots, \alpha_m\}$. It is easy to check that the $\mathbb{F}_q$-linear span of the set $\{(h_i(\alpha_1), \ldots, h_i(\alpha_m)) \mid 1 \leqslant i \leqslant m\}$ is the space $\mathbb{F}_q^m$ and $\max\{\deg h \mid h \in \mathcal{S}\} = \sum_{\alpha \in \mathcal{P}} \deg f_\alpha - \min\{\deg f_\alpha \mid \alpha \in \mathcal{P}\}$, where f_α is the minimal polynomial of α over $\mathbb{F}_q$.

Now we give our construction in a general framework. For a given positive integer n, assume that for some $m \geqslant n$ there exists a pair $(\hat{\mathcal{S}}, \hat{\mathcal{P}})$ such that $\hat{\mathcal{P}} = \{\alpha_1, \ldots, \alpha_m\}$ is a set of elements of $\overline{\mathbb{F}}_q$ with distinct minimal polynomials over $\mathbb{F}_q$ and $\hat{\mathcal{S}}$ is a set of m polynomials $h_1, \ldots, h_m \in \overline{\mathbb{F}}_q[x]$ such that the set

$$\{(h_i(\alpha_1), \ldots, h_i(\alpha_m)) \mid 1 \leqslant i \leqslant m\}$$

generates the space $\mathbb{F}_q^m$. Let f_i denote the minimal polynomial of α_i over $\mathbb{F}_q$ for $i = 1, \ldots, m$. Then it follows that $\max\{\deg h_i \mid 1 \leqslant i \leqslant m\} \geqslant \sum_{i=1}^m \deg f_i - \min\{\deg f_i \mid 1 \leqslant i \leqslant m\}$.

For example, let r be a prime number satisfying $(q^r - q)/r + q \geqslant n$ and let $m = (q^r - q)/r + q$. Consider the pair $(\mathcal{S}, \mathcal{P})$ as defined before. It is clear that $\hat{\mathcal{S}} = \mathcal{S}$ and $\hat{\mathcal{P}} = \mathcal{P}$ satisfy the conditions above.

We fix an order on $\hat{\mathscr{P}}$ as $\hat{\mathscr{P}} = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ and let $\hat{\mathscr{P}}_n = \{\alpha_1, \ldots, \alpha_n\}$. For $k \leqslant n$ and an $\mathbb{F}_q$-linearly independent subset $\{g_1, \ldots, g_k\} \subseteq \mathrm{Span}_{\mathbb{F}_q} \hat{\mathscr{S}}$ with the corresponding $k \times n$ matrix $G = (g_i(\alpha_j))_{1 \leqslant i \leqslant k, 1 \leqslant j \leqslant n}$ of full rank k, we denote the code generated by G as $C(g_1, \ldots, g_k; \hat{\mathscr{P}}_n)$. Note that when $m = n$, we have $C(h_1, \ldots, h_n; \hat{\mathscr{P}}_n) = \mathbb{F}_q^n$.

Example 2.2. Let $w \in \mathbb{F}_8$ with $w^3 = w + 1$. Let $\alpha_1 = 0$, $\alpha_2 = 1$, $\alpha_3 = w$, $\alpha_4 = w^3$ and $h_1 = 1$, $h_2 = x + x^2 + x^4$, $h_3 = x^3 + x^5 + x^6$, $h_4 = x^7$. Let $\hat{\mathscr{S}} = \{h_1, h_2, h_3, h_4\}$ and for each integer $1 \leqslant n \leqslant 4$ let $\hat{\mathscr{P}}_n = \{\alpha_1, \ldots, \alpha_n\}$. For instance we obtain $\mathbb{F}_2$-linear codes $C(h_1, h_2; \hat{\mathscr{P}}_4)$, which is a [4, 2, 2] code, and $C(h_1 + h_2 + h_3, h_4; \hat{\mathscr{P}}_3)$, which is a [3, 2, 2] code.

Remark 2.3. In [8], Xing and Ling considered the case $r = 2$ and they constructed codes with good parameters. Ling et al. [4] considered the general case that $r \geqslant 2$ is an integer. They constructed codes of arbitrary length and some codes with good parameters. In this remark we compare these constructions and our construction. We consider only a special type of our construction for the comparison. Namely, for a prime number r, we consider codes $C(h_1, \ldots, h_k; \hat{\mathscr{P}}_n)$ with $\{h_1, \ldots, h_k\} \subseteq \mathscr{S}$ and $\hat{\mathscr{P}} = \mathscr{P}$. Here $\mathscr{S}$ is the set of all associated polynomials $\{h_{\mathbf{a}} : \mathbf{a} \in \Lambda_q^r\}$and $\mathscr{P} \subset \mathbb{F}_{q^r}$ is a chosen subset of the largest cardinality satisfying (2.1) as defined above. Moreover, $\deg h_1 < \deg h_2 < \cdots < \deg h_k$ and $\deg h_k < \deg h$ for any $h \in \mathscr{S} \backslash \{h_1, \ldots, h_k\}$. Our special construction and the constructions in [8,4] are identical for $r = 2$. For $r \geqslant 3$ a prime integer, our special construction and the construction in [4] use similar subsets of $\mathbb{F}_{q^r}$ for evaluations of polynomials. For $r \geqslant 3$ a prime integer, the sets of polynomials used in our special construction and in [4] are different. For example, it can be readily verified that, when $q = 4$ and $r = 3$, the degrees of the largest set of polynomials used in [4] is a proper subset of the one in our special construction. The corresponding subset in our special construction includes the set of degrees {33, 49, 50, 54} as extra.

We observe that for $n \leqslant m$, any q-ary $[n, k, d]$ linear code C can be considered as $C(g_1, \ldots, g_k; \hat{\mathscr{P}}_n)$ uniquely upto an ordering of entries of $\hat{\mathscr{P}}$, for some $g_1, \ldots, g_k$.

Proposition 2.4. *Let the notation be as above. Given a q-ary $[n, k, d]$ linear code C, there exists a unique subspace $W_C = \langle g_1, \ldots, g_k \rangle \subseteq \mathrm{Span}_{\mathbb{F}_q} \hat{\mathscr{S}}$ such that $C = C(g_1, \ldots, g_k; \hat{\mathscr{P}}_n)$.*

Proof. We can embed $\iota : C \to \iota(C) \subseteq \mathbb{F}_q^m$ by appending zeroes. Since

$$\varphi : \mathrm{Span}_{\mathbb{F}_q} \hat{\mathscr{S}} \longrightarrow \mathbb{F}_q^m, \quad f \longmapsto (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_m))$$

is an $\mathbb{F}_q$-linear isomorphism, $W_C = \varphi^{-1}(\iota(C))$ is a uniquely determined linear subspace of $\mathrm{Span}_{\mathbb{F}_q} \hat{\mathscr{S}}$. The proof now follows from the definition of $C(g_1, \ldots, g_k; \hat{\mathscr{P}}_n)$. □

Hence for a prime number r, fixing an order on the elements of $\mathscr{P}$, we can find all q-ary linear codes of length $n \leqslant m = (q^r - q)/r + q$ in a unique way. Moreover, $m \to \infty$ as $r \to \infty$ for a fixed q.

For a given q-ary $[n, k, d]$ code $C(g_1, \ldots, g_k; \hat{\mathscr{P}}_n)$, the observation in Proposition 2.4 leads to a method for finding $g'_1, \ldots, g'_{n-k} \in \mathrm{Span}_{F_q} \hat{\mathscr{S}}$ explicitly such that $C(g_1, \ldots, g_k; \hat{\mathscr{P}}_n)^\perp = C(g'_1, \ldots, g'_{n-k}; \hat{\mathscr{P}}_n)$.

Theorem 2.5. *Let the notation be as above. Choose $g_{k+1}, \ldots, g_n \in \mathrm{Span}_{\mathbb{F}_q} \hat{\mathscr{S}}$ such that the $n \times n$ matrix $G = (g_i(\alpha_j))_{1 \leqslant i, j \leqslant n}$ is nonsingular. Consider the matrix B defined as*

$$B := (\mathbf{b}_1^t, \mathbf{b}_2^t, \ldots, \mathbf{b}_n^t) := (G^{-1})^t G^{-1},$$

where $\mathbf{b}_i = (\beta_{i,1}, \ldots, \beta_{i,n}) \in \mathbb{F}_q^n$ for $i = 1, 2, \ldots, n$. Let $g'_i \in \mathrm{Span}_{\mathbb{F}_q} \hat{\mathscr{S}}$ be defined as

$$g'_i = \beta_{k+i,1} g_1 + \beta_{k+i,2} g_2 + \cdots + \beta_{k+i,n} g_n$$

for $i = 1, 2, \ldots, n - k$. Then

$$C(g_1, \ldots, g_k; \hat{\mathscr{P}}_n)^\perp = C(g'_1, \ldots, g'_{n-k}; \hat{\mathscr{P}}_n).$$

Proof. Since B is invertible, $(\mathbf{b}_{k+1}^t, \mathbf{b}_{k+2}^t, \ldots, \mathbf{b}_n^t)$ is an $n \times (n-k)$ matrix of rank $n-k$. Hence $(g_i'(\alpha_j))_{1 \leqslant i \leqslant k, 1 \leqslant j \leqslant n}$ is a matrix of rank $n-k$ as well. Therefore, it is enough to prove that

$$g_i'(\alpha_1)g_j(\alpha_1) + g_i'(\alpha_2)g_j(\alpha_2) + \cdots + g_i'(\alpha_n)g_j(\alpha_n) = 0 \tag{2.2}$$

for $i = 1, 2, \ldots, n-k$ and $j = 1, 2, \ldots, k$. Note that by definition we have

$$(g_i'(\alpha_1), g_i'(\alpha_2), \ldots, g_i'(\alpha_n)) = \mathbf{b}_{k+i}G \tag{2.3}$$

for $i = 1, 2, \ldots, n-k$. Since

$$B^tG = \begin{pmatrix} \mathbf{b}_1 G \\ \mathbf{b}_2 G \\ \vdots \\ \mathbf{b}_n G \end{pmatrix} \quad \text{and} \quad (B^tG)G^t = I$$

by the definition of B, we have

$$(\mathbf{b}_i G)(g_j(\alpha_1), g_j(\alpha_2), \ldots, g_j(\alpha_n))^t = 0$$

for $0 \leqslant i, j \leqslant n$ and $i \neq j$. In particular

$$(\mathbf{b}_{k+i}G)(g_j(\alpha_1), g_j(\alpha_2), \ldots, g_j(\alpha_n))^t = 0$$

for $i = 1, 2, \ldots, n-k$ and $j = 1, 2, \ldots, k$ which is equivalent to (2.2) by using (2.3). This completes the proof. □

Remark 2.6. For $\hat{\mathscr{S}} = \{h_1, \ldots, h_m\}$ and $\hat{\mathscr{P}} = \{\alpha_1, \ldots, \alpha_m\}$, since the set

$$\{(h_i(\alpha_1), \ldots, h_i(\alpha_m)) | 1 \leqslant i \leqslant m\}$$

generates the $\mathbb{F}_q$-linear space $\mathbb{F}_q^m$, the codes in our construction can be considered as evaluation codes (see [3, Section 4]). Therefore, using filtrations of subspaces of $\mathrm{Span}_{\mathbb{F}_q}\hat{\mathscr{S}}$, we get lower bounds on the minimum distance of a given dual code $C(g_1, \ldots, g_k; \hat{\mathscr{P}}_n)^\perp$. For simplicity, we assume $n = m$ in this remark. Recall the $\mathbb{F}_q$-linear isomorphism

$$\varphi : \mathrm{Span}_{\mathbb{F}_q}\hat{\mathscr{S}} \longrightarrow \mathbb{F}_q^m, \qquad f \longmapsto (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_m)).$$

Let

$$\mathscr{F} : W_C = W_k \subset W_{k+1} \subset \cdots \subset W_n = \mathrm{Span}_{\mathbb{F}_q}\hat{\mathscr{S}},$$

be a filtration, where $W_C = \langle g_1, \ldots, g_k \rangle$ and $\dim_{\mathbb{F}_q} \varphi(W_i) = i$ for $k \leqslant i \leqslant n$. Every choice of such a filtration gives a lower bound on the minimum distance of $C(g_1, \ldots, g_k; \hat{\mathscr{P}}_n)^\perp$. Indeed, choose $\{g_{k+1}, \ldots, g_n\}$ such that $W_l = \mathrm{Span}_{\mathbb{F}_q}\{g_1, \ldots, g_l\}$ for $k \leqslant l \leqslant n$. We have the dual filtration $\mathscr{F}^\perp$ given as

$$\begin{aligned} \mathscr{F}^\perp : C(g_1, \ldots, g_k; \hat{\mathscr{P}}_n)^\perp &\supset C(g_1, \ldots, g_{k+1}; \hat{\mathscr{P}}_n)^\perp \supset \cdots \supset \{\mathbf{0}\} \\ &= C(g_1, \ldots, g_n; \hat{\mathscr{P}}_n)^\perp. \end{aligned}$$

Using the $\mathbb{F}_q$-linear isomorphism φ, we define $g_{ij} \in \mathrm{Span}_{\mathbb{F}_q}\hat{\mathscr{S}}$ such that $g_{ij}(\alpha) = g_i(\alpha)g_j(\alpha)$ for any $1 \leqslant i, j \leqslant n$. For $\mathbf{y} = (y_1, \ldots, y_n) \in C(g_1, \ldots, g_k; \hat{\mathscr{P}}_n)^\perp$ we define the following $n \times n$ matrices over $\mathbb{F}_q$:

$$M = (g_i(\alpha_j))_{1 \leqslant i,j \leqslant n}, \quad D = \mathrm{diag}(y_1, \ldots, y_n), \quad M_{\mathbf{y}} = (\mathbf{y} \cdot \varphi(g_{ij}))_{1 \leqslant i,j \leqslant n},$$

where D is the diagonal matrix with $y_1, y_2, \ldots, y_n$ as its entries in the main diagonal. Then $M_{\mathbf{y}} = MDM^t$ and hence for the Hamming weight $\mathrm{wt}(\mathbf{y})$ of the codeword $\mathbf{y} \in C(g_1, \ldots, g_k; \hat{\mathscr{P}}_n)^\perp$ we have

$$\mathrm{wt}(\mathbf{y}) = \mathrm{rank}\, D = \mathrm{rank}\, M_{\mathbf{y}}.$$

Moreover, it is possible to give nontrivial lower bounds on the rank of $M_{\mathbf{y}}$. If $\mathbf{y} \in C(g_1, \ldots, g_l; \hat{\mathscr{P}}_n)^{\perp} \backslash C(g_1, \ldots, g_{l+1}; \hat{\mathscr{P}}_n)^{\perp}$, then $\mathbf{y} \cdot \varphi(g_{ij}) = 0$ for $g_{ij} \in W_l$ and $\mathbf{y} \cdot \varphi(g_{ij}) \neq 0$ for $g_{ij} \in W_{l+1} \backslash W_l$. Using different filtrations we can get different lower bounds.

We illustrate Remark 2.6 in a simple example.

Example 2.7. Using the arguments in Remark 2.6, in this example we show that the dual $C(h_1, h_2; \hat{\mathscr{P}}_4)^{\perp}$ of the $\mathbb{F}_2$-linear [4, 2, 2] code $C(h_1, h_2; \hat{\mathscr{P}}_4)$ constructed in Example 2.2 is also a [4, 2, 2] code. We keep the notation of Example 2.2 and Remark 2.6. Let $g_i = h_i$ for $1 \leqslant i \leqslant 4$.

We use the filtration

$$\langle g_1, g_2 \rangle \subset \langle g_1, g_2, g_3 \rangle \subset \langle g_1, g_2, g_3, g_4 \rangle. \tag{2.4}$$

Note that $\hat{\mathscr{P}}_4$ is ordered as $\hat{\mathscr{P}}_4 = (0, 1, w, w^3)$. Then

$$\begin{aligned}
&\varphi(g_1) = [1, 1, 1, 1],\\
&\varphi(g_2) = [0, 1, 0, 1],\\
&\varphi(g_3) = [0, 1, 1, 0],\\
&\varphi(g_4) = [0, 1, 1, 1].
\end{aligned}$$

From the definition of $g_{i,j}$ for $1 \leqslant i, j \leqslant 4$, it follows that

$$\begin{aligned}
&g_{1,1} = g_1,\ g_{1,2} = g_{2,1} = g_2,\ g_{1,3} = g_{3,1} = g_3,\ g_{1,4} = g_{4,1} = g_4,\\
&g_{2,2} = g_2,\ g_{3,3} = g_3,\ g_{4,4} = g_4,\\
&g_{2,3} = g_{3,2} = g_2 + g_3 + g_4,\\
&g_{2,4} = g_{4,2} = g_2,\\
&g_{3,4} = g_{4,3} = g_3.
\end{aligned}$$

Using (2.4) we obtain that

$$\{\mathbf{0}\} = C(g_1, g_2, g_3, g_4; \hat{\mathscr{P}}_4)^{\perp} \subset C(g_1, g_2, g_3; \hat{\mathscr{P}}_4)^{\perp} \subset C(g_1, g_2; \hat{\mathscr{P}}_4)^{\perp}.$$

If $\mathbf{y} \in C(g_1, g_2, g_3; \hat{\mathscr{P}}_4)^{\perp} \backslash \{\mathbf{0}\}$, then by the argument in Remark 2.6, we have that

$$M_{\mathbf{y}} = \begin{bmatrix} 0 & 0 & 0 & * \\ 0 & 0 & * & 0 \\ 0 & * & 0 & 0 \\ * & 0 & 0 & * \end{bmatrix},$$

where $*$ denotes a nonzero entry (which is 1 in this case since the code is binary). Hence $\mathrm{wt}(\mathbf{y}) = 4$ for $\mathbf{y} \in C(g_1, g_2, g_3; \hat{\mathscr{P}}_4)^{\perp} \backslash \{\mathbf{0}\}$.

If $\mathbf{y} \in C(g_1, g_2; \hat{\mathscr{P}}_4)^{\perp} \backslash C(g_1, g_2, g_3; \hat{\mathscr{P}}_4)^{\perp}$, then

$$M_{\mathbf{y}} = \begin{bmatrix} 0 & 0 & * & ? \\ 0 & 0 & ? & 0 \\ * & ? & * & * \\ ? & 0 & * & ? \end{bmatrix},$$

where $*$ denotes a nonzero entry and ? denotes an entry whose value (zero or nonzero) we do not know. Hence $\mathrm{wt}(\mathbf{y}) \geqslant 2$ for $\mathbf{y} \in C(g_1, g_2; \hat{\mathscr{P}}_4)^{\perp}$. Therefore, $C(g_1, g_2; \hat{\mathscr{P}}_4)^{\perp}$ is an $\mathbb{F}_2$-linear [4, 2, 2] code since there is no $\mathbb{F}_2$-linear [4, 2, 3] code.

For the remainder of the paper, for a prime number r, we fix $\mathscr{S}$ to be the set of all associated polynomials $\{h_{\mathbf{a}} : \mathbf{a} \in \Lambda_q^r\}$ and $\hat{\mathscr{P}} = \mathscr{P}$ to be a chosen subset of $\mathbb{F}_{q^r}$ with the largest cardinality satisfying (2.1) as defined above.

Remark 2.8. In Section 2, we have chosen to introduce our codes using the general pair $(\hat{\mathscr{S}}, \hat{\mathscr{P}})$ instead of the constructive approach of the special class $(\mathscr{S}, \mathscr{P})$. This allows us to give some results in the more general context of $(\hat{\mathscr{S}}, \hat{\mathscr{P}})$, see for example Theorem 2.5.

3. Direct constructions of dual codes

Let r be a prime, $\mathbb{F}_q$ a finite field of characteristic different from r and $n = (q^r - q)/r + q$. In this section we study direct constructions of dual codes corresponding to pairs $(\mathscr{S}, \mathscr{P})$ defined in Section 2. We explicitly construct (quasi) self-orthogonal codes with good parameters. Throughout the section we order the elements of $\mathscr{S} = \{h_1, \ldots, h_n\}$ such that $\deg h_i < \deg h_{i+1}$ for $i = 1, \ldots, n-1$. Then we have $h_1 = 1$ and $h_n = x^{(q-1)(1+q+\ldots+q^{r-1})} = x^{q^r-1}$. Moreover, we also order the elements of $\mathscr{P}$ as $\mathscr{P} = (\alpha_1, \alpha_2, \ldots, \alpha_q, \alpha_{q+1}, \ldots, \alpha_n)$, where $\{\alpha_1, \ldots, \alpha_q\} = \mathbb{F}_q$.

Theorem 3.1. *Let $1 \leqslant k \leqslant n-1$. For any subset $\{h_{j_1}, \ldots, h_{j_k}\} \subseteq \mathscr{S}$ with $\{h_1, h_n\} \nsubseteq \{h_{j_1}, \ldots, h_{j_k}\}$ we have*

$$C(h_{j_1}, \ldots, h_{j_k}; \mathscr{P})^{\perp} = (\underbrace{1, \ldots, 1}_{q \text{ times}}, \underbrace{r, \ldots, r}_{n-q \text{ times}}) \cdot C(h'_{j_1}, \ldots, h'_{j_{n-k}}; \mathscr{P}),$$

where $\{h'_{j_1}, \ldots, h'_{j_{n-k}}\} = \mathscr{S} \backslash \{\overline{h}_{j_1}, \ldots, \overline{h}_{j_k}\}$. Moreover, if r is a square in $\mathbb{F}_q$ with $c^2 = r$ and $\overline{h}_{j_i} \notin \{h_{j_1}, \ldots, h_{j_k}\}$ for $i = 1, \ldots, k$, then

$$(\underbrace{1, \ldots, 1}_{q \text{ times}}, \underbrace{c, \ldots, c}_{n-q \text{ times}}) \cdot C(h_{j_1}, \ldots, h_{j_k}; \mathscr{P})$$

is self-orthogonal.

Proof. First note that $\sum_{\alpha \in \mathbb{F}_{q^r}} \alpha^i = 0$ for $0 \leqslant i \leqslant q^r - 2$. This is trivial for $i = 0$. For $1 \leqslant i \leqslant q^r - 2$, we can choose $c = c(i) \in \mathbb{F}_{q^r}$ such that $c^i \in \mathbb{F}_{q^r} \backslash \{0, 1\}$. Hence

$$\sum_{\alpha \in \mathbb{F}_{q^r}} \alpha^i = \sum_{\alpha \in \mathbb{F}_{q^r}} (c\alpha)^i = c^i \sum_{\alpha \in \mathbb{F}_{q^r}} \alpha^i.$$

Then

$$(1 - c^i) \sum_{\alpha \in \mathbb{F}_{q^r}} \alpha^i = 0 \quad \text{and} \quad \sum_{\alpha \in \mathbb{F}_{q^r}} \alpha^i = 0 \quad \text{since } 1 \neq c^i.$$

Therefore, if $h \in \mathbb{F}_q[x]$ and $\deg h \leqslant q^r - 2$, then

$$\sum_{\alpha \in \mathbb{F}_{q^r}} h(\alpha) = 0. \tag{3.1}$$

Since $\mathrm{Span}_{\mathbb{F}_q} \mathscr{S}$ forms a ring with multiplication modulo $(x^{q^r} - x)$ and $\mathscr{S}$ is a basis, we have for any $1 \leqslant i_1 \leqslant k$ and $1 \leqslant i_2 \leqslant n - k$, a uniquely determined $a_l(i_1, i_2) \in \mathbb{F}_q$ for $l = 1, \ldots, n$ satisfying

$$h_{j_{i_1}} h'_{j_{i_2}} \equiv \sum_{l=1}^{n} a_l(i_1, i_2) h_l \bmod (x^{q^r} - x). \tag{3.2}$$

Moreover, by the definition of the operation $h \mapsto \overline{h}$ on $\mathscr{S}$ and by the definition of the set $\{h'_{j_1}, \ldots, h'_{j_{n-k}}\}$, we have $a_n(i_1, i_2) = 0$ for $1 \leqslant i_1 \leqslant k$ and $1 \leqslant i_2 \leqslant n - k$. Therefore, since $h(\alpha) = h(\alpha^q)$ for any $h \in \mathrm{Span}_{\mathbb{F}_q} \mathscr{S}$ and $\alpha \in \mathbb{F}_{q^r}$, we get

$$\begin{aligned}&(h_{j_{i_1}}(\alpha_1), \ldots, h_{j_{i_1}}(\alpha_q), h_{j_{i_1}}(\alpha_{q+1}), \ldots, h_{j_{i_1}}(\alpha_n)) \\ &\quad \times (h'_{j_{i_2}}(\alpha_1), \ldots, h'_{j_{i_2}}(\alpha_q), r h'_{j_{i_2}}(\alpha_{q+1}), \ldots, r h'_{j_{i_2}}(\alpha_n)) = \sum_{\alpha \in \mathbb{F}_{q^r}} h_{j_{i_1}}(\alpha) h'_{j_{i_2}}(\alpha)\end{aligned}$$

for $1 \leqslant i_1 \leqslant k$ and $1 \leqslant i_2 \leqslant n-k$. Using (3.1) and (3.2) we complete the proof. □

It is possible to characterize the subsets $T \subset \mathscr{S}$ satisfying the property

$$\overline{h} \notin T \quad \text{for any } h \in T. \tag{3.3}$$

First, we determine the elements $\mathbf{a} \in \Lambda_q^r$ such that $\overline{O}_{\mathbf{a}} = O_{\mathbf{a}}$.

Proposition 3.2. *For $\mathbf{a} \in \Lambda_q^r$, we have the following equivalences depending on the cases.*
Case r is 2: $\overline{O}_{\mathbf{a}} = O_{\mathbf{a}} \Leftrightarrow \mathbf{a} = (a, b)$ with $a + b = q - 1$.
Case r is odd and q is even: $\overline{O}_{\mathbf{a}} \neq O_{\mathbf{a}}$ for any $\mathbf{a} \in \Lambda_q^r$.
Case r is odd and q is odd: $\overline{O}_{\mathbf{a}} = O_{\mathbf{a}} \Leftrightarrow \mathbf{a} = (a_1, \ldots, a_r)$ with $a_1 = \cdots = a_r = (q-1)/2$.

Proof. The case $r = 2$ directly follows from the definitions. First, we consider the case that r is odd and q is even. Assume the contrary, then there exists $\mathbf{a} = (a_1, \ldots, a_r) \in \Lambda_q^r$ such that, for all $0 \leqslant i \leqslant q-1$, we have

$$\#i\text{'s in } (a_1, \ldots, a_r) = \#(q-1-i)\text{'s in } (a_1, \ldots, a_r).$$

Therefore,

$$\begin{aligned} r &= \sum_{i=0}^{q-1} \#i\text{'s in } (a_1, \ldots, a_r) \\ &= 2 \sum_{i=0}^{q/2-1} \#i\text{'s in } (a_1, \ldots, a_r), \end{aligned}$$

which is a contradiction since r is odd.

Next we prove the remaining case that both r and q are odd. We note that the action of Ω_r on Λ_q^r induces an action on the set of indices $\{1, \ldots, r\}$ also.

Assume that $\overline{O}_{\mathbf{a}} = O_{\mathbf{a}}$ and let $I = \{i : 1 \leqslant i \leqslant r, \text{ and } a_i = (q-1)/2\}$. Then I is nonempty. Indeed otherwise we can apply the argument above and hence we get a contradiction to the fact that r is odd.

The assumption that $\overline{O}_{\mathbf{a}} = O_{\mathbf{a}}$ implies that $\overline{\mathbf{a}} = (q-1-a_1, \ldots, q-1-a_r) \in O_{\mathbf{a}}$, which means that there is some $1 \leqslant j \leqslant r$ such that

$$(q-1-a_1, \ldots, q-1-a_r) = \overline{\mathbf{a}} = \omega_r^j(\mathbf{a}) = \omega_r^j(a_1, \ldots, a_r). \tag{3.4}$$

For $i \in I$, we have $q-1-a_i = a_i$, so ω_r^j fixes I (when considered as acting on $\{1, \ldots, r\}$). It is well-known that the stabilizer of I in Ω_r is a subgroup of Ω_r. Since r is a prime, this stabilizer is either the trivial subgroup or the entire Ω_r.

Clearly, if the stabilizer of I is the trivial subgroup (i.e., $j = 0$ or, equivalently, $j = r$), then (3.4) shows that $a_1 = \cdots = a_r = (q-1)/2$. This, however, contradicts the assumption that the stabilizer of I is trivial.

Now suppose the stabilizer of I is Ω_r. Since I is nonempty, let $i \in I$ for some $1 \leqslant i \leqslant r$. Applying (3.4) shows that $q-1-a_{i-j} = a_1 = (q-1)/2$, so $a_{i-j} = (q-1)/2$, for all $1 \leqslant j \leqslant r$. (Here, the indices of a_{i-j} are taken modulo r.) This shows again that $a_1 = \cdots = a_r = (q-1)/2$. □

Next we define special subsets S_0, S_-, and S_+ depending on the cases.
Case r is 2 and q is odd:

$$\begin{aligned} S_0 &= \{h_{\mathbf{a}} \in \mathscr{S} \mid \mathbf{a} = (a, b) \text{ with } a + b = q - 1\}, \\ S_- &= \{h_{\mathbf{a}} \in \mathscr{S} \mid \mathbf{a} = (a, b) \text{ with } a + b < q - 1\}, \\ S_+ &= \{h_{\mathbf{a}} \in \mathscr{S} \mid \mathbf{a} = (a, b) \text{ with } a + b > q - 1\}. \end{aligned}$$

Case r is odd and q is even:

$$
\begin{aligned}
&S_0 = \emptyset,\\
&S_- = \left\{ h_{\mathbf{a}} \in \mathscr{S} \mid \mathbf{a} = (a_1, \ldots, a_r) \text{ and } \sum_{i=0}^{q/2-1} \#i\text{'s in } \mathbf{a} < \sum_{i=q/2}^{q-1} \#i\text{'s in } \mathbf{a} \right\},\\
&S_+ = \left\{ h_{\mathbf{a}} \in \mathscr{S} \mid \mathbf{a} = (a_1, \ldots, a_r) \text{ and } \sum_{i=0}^{q/2-1} \#i\text{'s in } \mathbf{a} > \sum_{i=q/2}^{q-1} \#i\text{'s in } \mathbf{a} \right\}.
\end{aligned}
$$

Case r is odd and q is odd: For simplicity we consider $r = 3$ and let $\mathbf{s} = ((q-1)/2, (q-1)/2, (q-1)/2) \in \Lambda_q^3$.

$$
\begin{aligned}
&S_0 = \{h_{\mathbf{s}}\},\\
&S_- = \left\{ h_{\mathbf{a}} \in \mathscr{S} \mid \mathbf{a} = (a_1, a_2, a_3) \text{ and } \sum_{i=0}^{(q-1)/2-1} \#i\text{'s in } \mathbf{a} < \sum_{i=(q-1)/2+1}^{q-1} \#i\text{'s in } \mathbf{a} \right\}\\
&\qquad \cup \left\{ h_{\mathbf{i}} \in \mathscr{S} \mid \mathbf{i} = \left(\frac{q-1}{2}, i, q-1-i \right) \text{ and } i < \frac{q-1}{2} \right\},\\
&S_+ = \left\{ h_{\mathbf{a}} \in \mathscr{S} \mid \mathbf{a} = (a_1, a_2, a_3) \text{ and } \sum_{i=0}^{(q-1)/2-1} \#i\text{'s in } \mathbf{a} > \sum_{i=(q-1)/2+1}^{q-1} \#i\text{'s in } \mathbf{a} \right\}\\
&\qquad \cup \left\{ h_{\mathbf{i}} \in \mathscr{S} \mid \mathbf{i} = \left(\frac{q-1}{2}, i, q-1-i \right) \text{ and } i > \frac{q-1}{2} \right\}.
\end{aligned}
$$

For a subset $T \subset \mathscr{S}$, we denote by $\overline{T}$ the subset $\{\overline{h} \mid h \in T\}$.

Theorem 3.3. *Let the notation be as above. Then* $\mathscr{S} = S_0 \sqcup S_- \sqcup S_+$, $\#S_- = \#S_+$ *and* $T \subset \mathscr{S}$ *satisfies* (3.3) *if and only if*

$$
\overline{(T \cap S_-)} \cap (T \cap S_+) = \emptyset \quad \text{and} \quad T \cap S_0 = \emptyset. \tag{3.5}
$$

Proof. It is easy to observe that, in each case, $\mathscr{S} = S_0 \sqcup S_- \sqcup S_+$. Moreover, $h_{\mathbf{a}} \in S_-$ if and only if $\overline{h}_{\mathbf{a}} \in S_+$ by definition. Hence $\overline{S}_- = S_+$ and $\#S_- = \#S_+$ in each case. The equivalence of the conditions (3.3) and (3.5) is now clear from the definitions. □

Note that in the case r is odd and q is even, for $T \subset \mathscr{S}$ satisfying (3.5) and $\#T = n/2$ we obtain self-dual codes. We obtain similar results for the pair $(\widetilde{\mathscr{S}}, \widetilde{\mathscr{P}})$ where

$$
\widetilde{\mathscr{S}} = \mathscr{S} \backslash \{h_n\} \quad \text{and} \quad \widetilde{\mathscr{P}} = (\alpha_2, \alpha_3, \ldots, \alpha_n),
$$

where $\alpha_1 = 0$. Let $\tilde{n} = n - 1 = (q^r - q)/r + q - 1$ and define

$$
\begin{aligned}
&\widetilde{\overline{h}}_i = \overline{h}_i \quad \text{if } 2 \leqslant i \leqslant n-1,\\
&\widetilde{\overline{h}}_1 = h_1.
\end{aligned}
$$

Theorem 3.4. *Let $1 \leqslant k \leqslant \tilde{n} - 1$. For any subset $\{h_{j_1}, \ldots, h_{j_k}\} \subseteq \widetilde{\mathscr{S}}$ we have*

$$C(h_{j_1}, \ldots, h_{j_k}; \widetilde{\mathscr{P}})^{\perp} = (\underbrace{1, \ldots, 1}_{q-1 \text{ times}}, \underbrace{r, \ldots, r}_{n-q \text{ times}}) \cdot C(h'_{j_1}, \ldots, h'_{j_{n-1-k}}; \widetilde{\mathscr{P}}), \tag{3.6}$$

where $\{h'_{j_1}, \ldots, h'_{j_{n-1-k}}\} = \widetilde{\mathscr{S}} \backslash \{\widetilde{\overline{h}}_{j_1}, \ldots, \widetilde{\overline{h}}_{j_k}\}$. Furthermore, if r is a square in $\mathbb{F}_q$ with $c^2 = r$ and $\widetilde{\overline{h}}_{j_i} \notin \{h_{j_1}, \ldots, h_{j_k}\}$ for $i = 1, \ldots, k$, then

$$(\underbrace{1, \ldots, 1}_{q-1 \text{ times}}, \underbrace{c, \ldots, c}_{n-q \text{ times}}) \cdot C(h_{j_1}, \ldots, h_{j_k}; \widetilde{\mathscr{P}}) \tag{3.7}$$

is self-orthogonal. Moreover, let $T \subset \mathscr{S}$ be a subset with $h_1 \in T$ satisfying (3.5). *If $C(T, \mathscr{P})$ is a q-ary $[n, k, d]$ code, then the code $(1, \ldots, 1, c, \ldots, c) \cdot C(T \backslash \{h_1\}; \widetilde{\mathscr{P}})$ is a (quasi) self-orthogonal q-ary $[n-1, k-1, d_1]$ code with $d_1 \geqslant d$.*

Proof. First, note that $\overline{h}_i \neq h_1$ for any $2 \leqslant i \leqslant n-1$. Then

$$\{h'_{j_1}, \ldots, h'_{j_{n-1-k}}\} \subseteq \mathscr{S} \backslash \{h_{j_1}, \ldots, h_{j_k}\}.$$

Next we observe that

$$h_1(\alpha) = h_n(\alpha) \quad \text{for any } \alpha \in \widetilde{\mathscr{P}}$$

and

$$h_i(\alpha_1) = 0 \quad \text{for } 2 \leqslant i \leqslant n-1.$$

Therefore, for any $1 \leqslant i_1 \leqslant k$ and $1 \leqslant i_2 \leqslant n-1-k$, we have

$$\begin{aligned}
&(h_{j_{i_1}}(\alpha_2), \ldots, h_{j_{i_1}}(\alpha_q), h_{j_{i_1}}(\alpha_{q+1}), \ldots, h_{j_{i_1}}(\alpha_n)) \\
&\quad \times (h'_{j_{i_2}}(\alpha_2), \ldots, h'_{j_{i_2}}(\alpha_q), rh'_{j_{i_2}}(\alpha_{q+1}), \ldots, rh'_{j_{i_2}}(\alpha_n)) \\
&\quad = (h_{j_{i_1}}(\alpha_1), \ldots, h_{j_{i_1}}(\alpha_q), h_{j_{i_1}}(\alpha_{q+1}), \ldots, h_{j_{i_1}}(\alpha_n)) \\
&\quad \times (h'_{j_{i_2}}(\alpha_1), \ldots, h'_{j_{i_2}}(\alpha_q), rh'_{j_{i_2}}(\alpha_{q+1}), \ldots, rh'_{j_{i_1}}(\alpha_n)) \\
&\quad = \sum_{\alpha \in \mathbb{F}_{q^r}} h_{j_{i_1}}(\alpha) h'_{j_{i_2}}(\alpha).
\end{aligned}$$

Using the arguments in the proof of Theorem 3.1, we obtain (3.6) and (3.7).

Next we assume that $T \subset \mathscr{S}$ with $h_1 \in T$ satisfying (3.5). Then $C(T \backslash \{h_1\}; \mathscr{P})$ is a subcode of $C(T; \mathscr{P})$ and hence the minimum distance of $C(T \backslash \{h_1\}; \mathscr{P})$ is at least d. Moreover, for any $h \in T \backslash \{h_1\}$, we have $h(\alpha_1) = 0$ and therefore $d_1 \geqslant d$. Also (quasi) self-orthogonality follows from the definition of T. This completes the proof. □

Note that in the case r is odd and q is odd, $\#S_0 = 1$. Moreover, let $q \equiv 1 \bmod 4$ and hence choose $e \in \mathbb{F}_q$ with $e^2 = -1$. Then we can get (quasi) self-dual codes using $\widetilde{\mathscr{P}}$ as follows. For simplicity, we assume that $r = 3$.

Theorem 3.5. *Let $\mathbb{F}_q$ be a finite field with $q \equiv 1 \bmod 4$, $e \in \mathbb{F}_q$ with $e^2 = -1$, $r = 3$ and $\mathbf{s} = ((q-1)/2, (q-1)/2, (q-1)/2) \in \Lambda_q^3$. Let $T \subset \mathscr{S}$ be a subset with $h_1, h_{\mathbf{s}} \in T$ and $T \backslash \{h_{\mathbf{s}}\}$ satisfying* (3.5). *Let $T_1 = T \cup \{eh_1 + h_{\mathbf{s}}\} \backslash \{h_1, h_{\mathbf{s}}\}$. If $C(T, \mathscr{P})$ is a q-ary $[n, k, d]$ code, then*

$$(1, \ldots, 1, c, \ldots, c) \cdot C(T_1, \widetilde{\mathscr{P}})$$

is a (quasi) self-orthogonal q-ary $[n-1, k-1, d_1]$ code with $d_1 \geqslant d$. In particular it is (quasi) self-dual when $k = (n-1)/2 + 1$.

Proof. Note that $(h_{\mathbf{s}}(\alpha))^2 = h_n(\alpha)$ for any $\alpha \in \mathbb{F}_{q^3}$ and hence

$$\sum_{\alpha\in\mathbb{F}_{q^3}\setminus\{0\}} (h_{\mathbf{s}}(\alpha))^2 = \sum_{\alpha\in\mathbb{F}_{q^3}\setminus\{0\}} 1 = -1.$$

Then

$$\begin{aligned}
&\sum_{\alpha\in\mathbb{F}_{q^3}\setminus\{0\}} ((eh_1 + h_{\mathbf{s}})(\alpha))^2 \\
&= \sum_{\alpha\in\mathbb{F}_{q^3}\setminus\{0\}} e^2 + 2e \sum_{\alpha\in\mathbb{F}_{q^3}\setminus\{0\}} h_{\mathbf{s}}(\alpha) + \sum_{\alpha\in\mathbb{F}_{q^3}\setminus\{0\}} (h_{\mathbf{s}}(\alpha))^2 \\
&= e^2(-1) + 2e(0) + (-1) \\
&= 0.
\end{aligned}$$

The rest of the proof is similar to the proof of Theorem 3.1 □

Example 3.6. Using Theorem 3.1 and subsets $\{h_{j_1}, \ldots, h_{j_k}\} \subset \mathscr{S}$ satisfying (3.5) with $\deg h_{j_1} < \deg h_{j_2}$ for $1 \leqslant j_1 < j_2 \leqslant n$ and $\deg h_{j_k}$ as small as possible, we obtain the following (quasi) self-orthogonal q-ary $[n, k, d]$ codes whose parameters are the same as the best known ones for linear codes (see [2]). The minimum distances can be estimated as in [8] and using Magma [1].

$q = 2$: [4, 2, 2], [8, 4, 4],
$q = 3$: [6, 2, 4],
$q = 5$: [15, 2, 12], [15, 3, 11], [45, 3, 35], [45, 4, 34], [45, 10, 24], [45, 17, 17],
$q = 7$: [28, 2, 24], [28, 3, 23], [28, 5, 19], [28, 8, 15], [28, 9, 14],
$q = 9$: [45, 2, 40], [45, 3, 39], [45, 6, 33], [45, 7, 30], [45, 8, 29], [45, 9, 28], [45, 10, 27].

Using Theorem 3.4 and similar subsets of $\mathscr{S}$ we obtain the following (quasi) self-orthogonal q-ary $[n, k, d]$ codes whose parameters are the same as the best known ones for linear codes.

$q = 2$: [7, 3, 4],
$q = 5$: [14, 2, 11], [44, 16, 17],
$q = 7$: [27, 2, 23],
$q = 9$: [44, 2, 39], [44, 7, 29], [44, 8, 28], [44, 9, 27].

We also obtain some good (quasi) self-orthogonal codes whose parameters are beyond the range of Brouwer's tables ([2]).

$q = 8$: [176, 10, 127], [176, 9, 127],
$q = 11$: [66, 3, 59], [66, 6, 52], [66, 10, 45], [65, 2, 59], [65, 5, 52], [65, 9, 45].

We give a generator matrix for 5-ary quasi-self-orthogonal code [45, 17, 17] in Fig. 1

.

$$P = \begin{pmatrix}
4 & 3 & 1 & 4 & 2 & 4 & 1 & 4 & 1 & 0 & 3 & 4 & 4 & 3 & 3 & 1 & 3 & 1 & 2 & 1 & 1 & 3 & 0 & 4 & 3 & 1 & 1 & 1 \\
0 & 2 & 0 & 3 & 3 & 0 & 1 & 4 & 2 & 0 & 4 & 1 & 1 & 2 & 2 & 0 & 1 & 2 & 0 & 4 & 3 & 3 & 4 & 2 & 1 & 2 & 2 & 4 \\
1 & 2 & 2 & 3 & 0 & 1 & 2 & 1 & 4 & 3 & 3 & 0 & 1 & 4 & 4 & 0 & 1 & 3 & 4 & 1 & 3 & 2 & 2 & 2 & 2 & 3 & 4 & 0 \\
4 & 3 & 2 & 2 & 0 & 3 & 1 & 0 & 1 & 0 & 0 & 3 & 1 & 3 & 0 & 4 & 4 & 2 & 1 & 2 & 0 & 3 & 0 & 4 & 2 & 0 & 1 & 2 \\
0 & 2 & 4 & 2 & 1 & 0 & 3 & 3 & 2 & 0 & 3 & 2 & 1 & 3 & 3 & 4 & 3 & 1 & 0 & 1 & 2 & 1 & 3 & 1 & 1 & 4 & 1 & 2 \\
2 & 0 & 1 & 3 & 2 & 3 & 2 & 2 & 4 & 3 & 4 & 1 & 1 & 0 & 1 & 4 & 3 & 1 & 3 & 0 & 3 & 4 & 1 & 3 & 3 & 2 & 4 & 4 \\
2 & 3 & 2 & 1 & 2 & 2 & 4 & 3 & 1 & 4 & 1 & 1 & 2 & 2 & 1 & 0 & 4 & 4 & 0 & 2 & 0 & 4 & 0 & 3 & 3 & 2 & 0 & 1 \\
2 & 2 & 1 & 3 & 4 & 4 & 1 & 3 & 3 & 2 & 1 & 4 & 4 & 2 & 4 & 3 & 1 & 0 & 1 & 4 & 2 & 4 & 0 & 1 & 1 & 0 & 2 & 0 \\
4 & 1 & 3 & 0 & 0 & 3 & 4 & 0 & 0 & 0 & 1 & 3 & 1 & 2 & 4 & 1 & 3 & 0 & 0 & 0 & 4 & 1 & 3 & 2 & 3 & 3 & 3 & 0 \\
1 & 2 & 3 & 2 & 2 & 4 & 4 & 0 & 3 & 2 & 2 & 0 & 3 & 4 & 0 & 3 & 3 & 2 & 2 & 1 & 3 & 4 & 2 & 0 & 3 & 0 & 2 & 2 \\
2 & 4 & 3 & 3 & 4 & 2 & 3 & 2 & 0 & 1 & 3 & 1 & 3 & 4 & 3 & 4 & 0 & 1 & 1 & 0 & 1 & 1 & 4 & 2 & 3 & 2 & 4 & 3 \\
3 & 4 & 3 & 3 & 3 & 0 & 2 & 2 & 4 & 0 & 4 & 0 & 2 & 0 & 1 & 3 & 4 & 4 & 2 & 3 & 2 & 0 & 3 & 2 & 1 & 0 & 1 & 3 \\
2 & 4 & 4 & 1 & 2 & 1 & 2 & 3 & 3 & 2 & 2 & 1 & 0 & 1 & 0 & 2 & 3 & 1 & 0 & 2 & 1 & 3 & 1 & 1 & 2 & 4 & 4 & 2 \\
4 & 3 & 3 & 2 & 4 & 3 & 4 & 0 & 1 & 0 & 4 & 4 & 0 & 3 & 2 & 1 & 0 & 3 & 2 & 3 & 3 & 3 & 2 & 3 & 2 & 2 & 4 & 4 \\
2 & 3 & 1 & 4 & 2 & 2 & 2 & 1 & 1 & 4 & 4 & 2 & 3 & 0 & 3 & 3 & 4 & 1 & 4 & 4 & 4 & 0 & 2 & 1 & 4 & 3 & 4 & 1 \\
3 & 0 & 1 & 0 & 4 & 3 & 0 & 0 & 3 & 1 & 4 & 0 & 3 & 0 & 1 & 3 & 1 & 0 & 0 & 0 & 2 & 2 & 3 & 2 & 1 & 4 & 2 & 1 \\
0 & 3 & 2 & 0 & 1 & 1 & 0 & 3 & 3 & 4 & 3 & 4 & 1 & 3 & 4 & 0 & 3 & 0 & 4 & 3 & 2 & 3 & 1 & 3 & 1 & 4 & 2 & 1
\end{pmatrix}.$$

Fig. 1. A generator matrix G for 5-ary quasi self-orthogonal [45,17,17] code.

By applying the propagation rules (see, for example, [7, Exercise 1.2.24]), we get a 5-ary code [44, 17, 16], which is also a linear code with the best known parameters.

$$G := (I_{17} \mid P)_{17\times 45},$$

where I_{17} is the 17×17 identity matrix and P is a 17×28 matrix given in Fig. 1.

Remark 3.7. Example 3.6 as well as examples in [8] suggest that certain choices of r, subsets of $\mathscr{P}$ and subsets of $\mathscr{S}$ can yield good codes. It would be interesting to characterize some classes of good codes using our construction.

Acknowledgements

A part of this paper was written while the second author was visiting the Institute for Mathematical Sciences, National University of Singapore, Republic of Singapore. He would like to thank the institute for the support. The first and third authors are partially supported by MOE-ARF research Grant R-146-000-029-112 and DSTA research Grant R-394-000-011-422. The second author is partially supported by the Turkish Academy of Sciences in the framework of Young Scientists Award Programme (F.Ö./TÜBA-GEBIP/2003-13).

The authors would like to thank the anonymous referees for their detailed comments which led to better exposition.

References

[1] W. Bosma, J. Cannon, C. Playoust, The magma algebra system I: the user language, J. Symb. Comp. 24 (3–4) (1997) 235–265.
[2] A. Brouwer, Bounds on minimum distance of linear codes, ⟨http://www.win.tue.nl/∼aeb/voorlincod.html⟩, version of August 2, 2003.
[3] T. Høholdt, J.H. van Lint, R. Pellikaan, Algebraic geometry codes, in: V.S. Pless, W.C. Huffman, R.A. Brualdi (Eds.), Handbook of Coding Theory, North-Holland, Amsterdam, 1998.
[4] S. Ling, H. Niederreiter, C.P. Xing, Symmetric polynomials and some good codes, Finite Fields Appl. 7 (1) (2001) 142–148.
[5] H. Niederreiter, C.P. Xing, Rational Points on Curves over Finite fields—Theory and Application, London Mathematical Society, Lecture Note Series, vol. 285, Cambridge, 2001.
[6] R.R. Nielsen, Decoding the Xing-Ling codes, preprint, 2001.
[7] M.A. Tsfasman, S. Vlăduţ, Algebraic-Geometric Codes, Dordrecht, Kluwer, 1991.
[8] C.P. Xing, S. Ling, A class of linear codes with good parameters, IEEE Trans. Inform. Theory 46 (6) (2000) 2184–2188.
[9] C.P. Xing, S. Ling, A class of linear codes with good parameters from algebraic curves, IEEE Trans. Inform. Theory 46 (4) (2000) 1527–1532.